Эллиптические кривые

Лекция 1. Введение

Семён Новосёлов
на основе курса Елены Киршановой

БФУ им. И. Канта

2020

IKBFU

Мотивация

Криптография:

- классическая – дискретный логарифм (ECDH, ECDSA)
  - использование: https (TLS), SSH, IPsec
- постквантовая – изогении (SIKE)
  - кандидат на стандартизацию

Определение

$\mathbb{F}_q$ – конечное поле, $|\mathbb{F}_q| = q = p^n$, K – поле, $\overline{K}$ – алг. замыкание.

Уравнение Вейерштрасса в проективных координатах:

$$F : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad (1)$$

где $a_i \in K$.

- сингулярное: $\exists P \in \mathbb{P}^2(K) : \frac{dF}{dX}(P) = \frac{dF}{dY}(P) = \frac{dF}{dZ}(P) = 0$.
- гладкое (или несингулярное) в противном случае.

Эллиптическая кривая E – множество точек $\mathbb{P}^2(K)$, удовлетворяющих гладкой кривой (1).

- Точка в бесконечности: $\exists!\mathcal{O} = (0 : 1 : 0)$.

Уравнение Вейерштрасса **в аффинных координатах** $(x = X/Z, y = Y/Z)$:

$$f : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (2)$$

Тогда $E(K) = \{(x, y) \in K \times K : f(x, y) = 0\} \cup \{\mathcal{O}\}$.

- Проективные координаты позволяют избежать деления в арифметике за счёт доп. умножений.

Дискриминант

Обозначим

$$
\begin{aligned}
d_2 &= a_1^2 + 4a_2 \\
d_4 &= 2a_4 + a_1 a_3 \\
d_6 &= a_3^2 + 4a_6 \\
d_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\
c_4 &= d_2^2 - 24 d_4
\end{aligned}
\tag{3}
$$

Тогда **дискриминант** уравнения (2) определяется как

$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6.$$

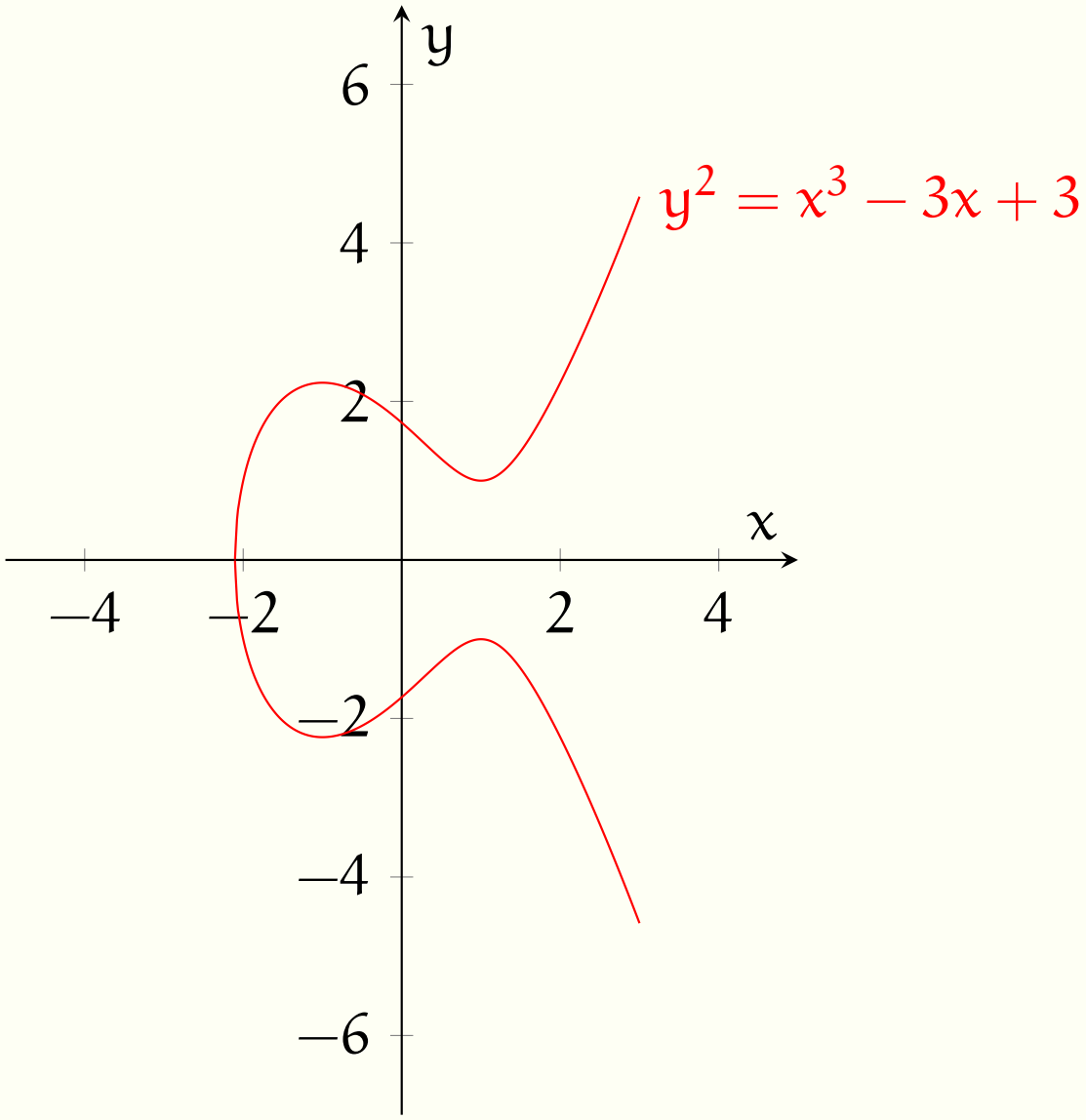
Классификация уравнений Вейерштрасса

Теорема [Silverman, Thm. 1.4]

1. $\Delta \neq 0 \iff$ кривая гладкая ($\implies$ задаёт эллиптическую кривую)
2. $\Delta = 0, c_4 \neq 0 \iff$ кривая обладает узлом (node)
3. $\Delta = c_4 = 0 \iff$ кривая обладает точкой перегиба (cusp)

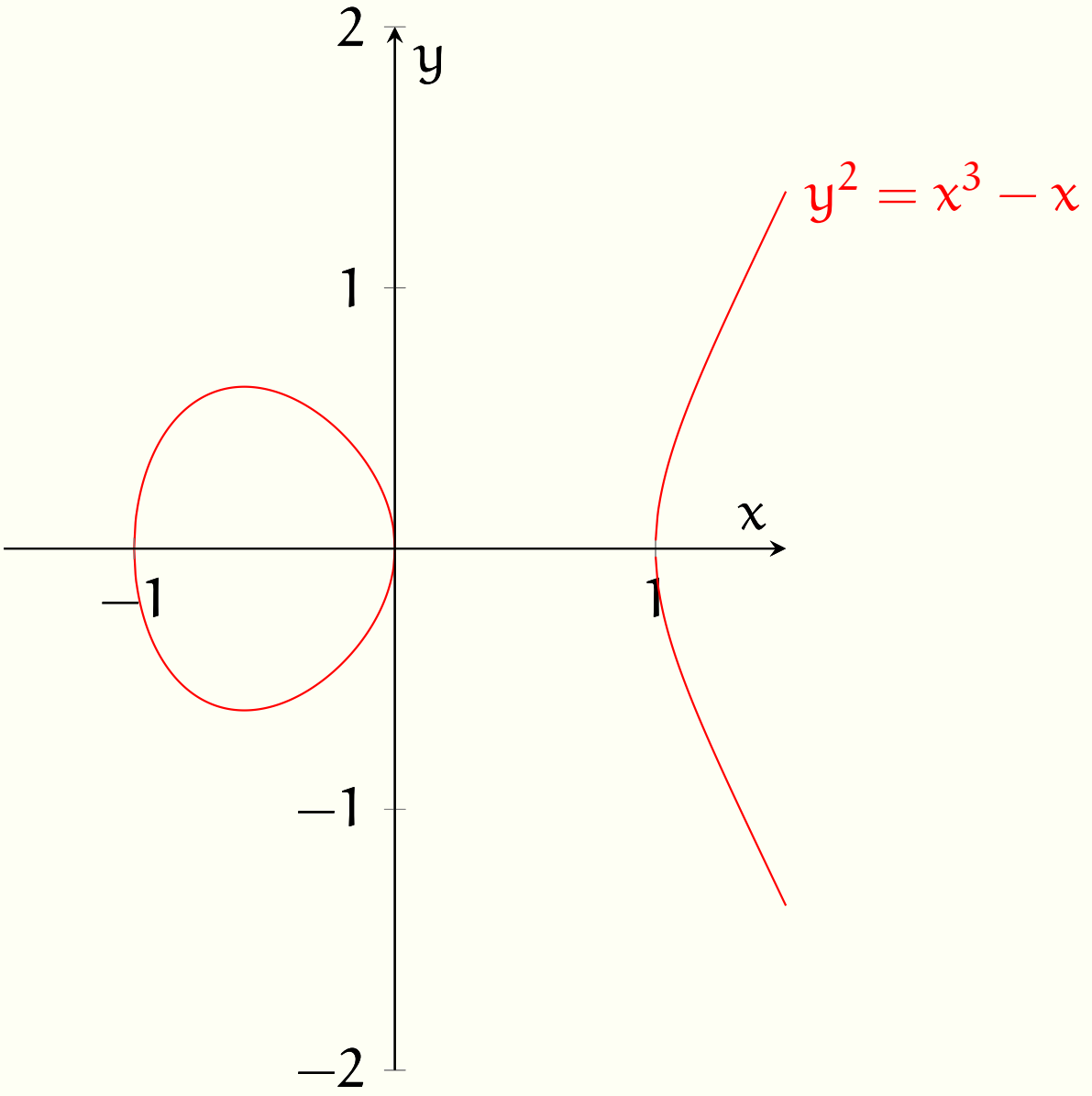
Классификация уравнений Вейерштрасса - 2

$\Delta < 0$



Классификация уравнений Вейерштрасса - 3

$\Delta > 0$



Изоморфизмы эллиптических кривых

Пусть $E_1/K, E_2/K$ – эллиптические кривые с уравнениями:

$$\begin{aligned} E_1 &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E_2 &: y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \end{aligned} \tag{4}$$

$E_1/K, E_2/K$ **изоморфны**, если они изоморфны как проективные многообразия.

Теорема

$E_1 \cong E_2 \iff \exists u, r, s, t \in K, u \neq 0$ такие, что замена

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \tag{5}$$

преобразует кривую E_1 в E_2.

Изоморфизм кривых задаёт отношение эквивалентности.

Краткие формы

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (2)$$

$charK \neq 2$: Изоморфизм

$$(x, y) \mapsto \left(x, \frac{1}{2}(y - a_1x - a_3)\right)$$

преобразует E/K к виду:

$$E/K : y^2 = 4x^3 + d_2x^2 + 2d_4 + d_6. \qquad (6)$$

$charK \neq 2, 3$: Изоморфизм

$$(x, y) \mapsto \left(\frac{x - 3d_2}{36}, \frac{y}{216}\right)$$

Преобразует (6) к виду:

$$E/K : y^2 = x^3 + ax + b \qquad (7)$$

$$a = -27c_4$$

$$b = -56(d_2^3 + 36d_2d_4 - 216d_6)$$

Краткие формы - 2

В последнем случае,

$$\Delta = -16(4a^3 + 27b^2)$$

$\mathrm{char}K = 2$:

$$a_1 \neq 0 \implies (x, y) \mapsto \left(a_1^2 x + \frac{a_3}{a_1}; a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$$

$$E/K : y^2 + xy = x^3 + a_2' x^2 + a_6' \tag{8}$$

$$a_1 \neq 0 \implies (x, y) \mapsto (x + a_2, y)$$

$$E/K : y^2 + a_3 y = x^3 + a_4 x + a_6 \tag{9}$$

Определение изоморфности кривых.

j-инвариант эллиптической кривой E:

$$j(E) = \frac{c_4^3}{\Delta}$$

или для краткой формы $j(E) = -1728\frac{4a^3}{\Delta}$.

Теорема

$E_1 \cong E_2$ над $\overline{K} \iff j(E_1) = j(E_2)$

Определение изоморфности кривых над полем K: проверка условий теоремы. Если выполняется – составление и решение системы уравнений используя (5).

Литература

1. Washington L.C. ”Elliptic curves number theory and cryptography”
2. Menezes A. ”Elliptic curve public key cryptosystems”
3. Hankerson D., Menezes A., Vanstone S. ”Guide to elliptic curve cryptography”
4. Blake I., Seroussi G., Smart N. ”Elliptic Curves in Cryptography”
5. Silverman J.H. ”The Arithmetic of Elliptic Curves”

Контакты

snovoselov@kantiana.ru